AFFIDAVIT OF SPECIAL AGENT LAURA MACRORIE IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Special Agent Laura Macrorie, being duly sworn, hereby state the following:

1. I am a federal law enforcement officer within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request arrest warrants and search warrants. I am currently employed as a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since March 2020. I have received twenty-one weeks' formal training in investigative techniques at the FBI Academy in Quantico, Virginia. I have also received training from the FBI Cyber Division in basic networking, mobile communications, analysis of digital records, social media, cloud communications, and email tracing.

2. Over the course of my career outside the FBI, I have worked with victims of human trafficking, domestic violence, kidnapping, and other violent crimes, where I have observed various forms of abuse that include manipulation and exploitation involving digital devices.

3. I am currently assigned to the Cyber Crimes Squad in the FBI's Boston Division. I am responsible for investigations involving computer system intrusions, internet fraud, and cyberstalking. I have participated in the execution of warrants involving cyber, white-collar, and violent crimes. Based on my training and experience, I am familiar with the means by which individuals use computers and information networks to commit these and other crimes. I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and I am accordingly empowered by law to conduct investigations and to make arrests for federal felony offenses. I am also a federal law enforcement officer within the meaning of Fed. R. Crim. P. 41(a)(2)(C), that is, a government agent authorized to enforce criminal laws and duly authorized by the Attorney General to request search warrants.

PURPOSE OF AFFIDAVIT

4. The FBI is currently investigating Jason SUBIRANA (DOB: xx/xx/1977) ("SUBIRANA") for cyberstalking, in violation of 18 U.S.C. § 2261A(2)(B) (the "Target Offense").

5. I make this affidavit in support of an application for search warrants for the premises located at [redacted], Dover, New Hampshire, 03820, a 2014 Infiniti Q50 (NH [redacted]), a 2015 Porsche 911 (NH [redacted]), and a 2019 Volvo V90 (NH [redacted]), three (3) vehicles registered to SUBIRANA, and for the person of Jason SUBIRANA (together, the "Target Locations"), as described in Attachments A-1, A-2, A-3, A-4, and A-5 and incorporated herein by reference, and to seize evidence, instrumentalities, fruits of crime, and contraband as more fully described in Attachment B, also incorporated herein by reference.

The facts stated herein are based on my own personal involvement in the below-described investigation, as well as from information provided by other law enforcement officers and from certain records. In submitting this affidavit, I have not included each and every fact known to me about this investigation; rather, I am only submitting enough evidence necessary to establish the requisite probable cause, including any mitigating information of which I am aware.

STATEMENT OF PROBABLE CAUSE

A. Background of Investigation

6. Since July of 2021, the FBI has been investigating Jason SUBIRANA ("SUBIRANA"), a resident of New Hampshire. The investigation centered on SUBIRANA's ongoing harassment of his then-girlfriend, Victim 1,[1] beginning almost immediately after they started dating in September 2020. Beginning in December 2020, Victim 1 received approximately 318 text messages via anonymized phone numbers intended to stalk, intimidate, shame, or otherwise cause her substantial emotional distress.

[1] Victim 1's identity is known to the FBI and has not been added to this affidavit to protect her identity.

7. The investigation to date has revealed SUBIRANA used voice over IP ("VOIP") services to obfuscate his identity and perpetrate the abuse. Specifically, SUBIRANA is known to have used at least nine (9) VOIP accounts from TextNow, Inc.[2] to further his scheme. The FBI is also aware of at least six (6) additional TextNow accounts associated with SUBIRANA, which are likely being used in furtherance of his criminal activity.

8. SUBIRANA also contacted numerous friends, family, and associates of Victim 1 via TextNow phone numbers and anonymous mail to defame, and further isolate her from her support system. For example, Victim 1's neighbor received a print-out in the mail of a text message exchange in which Victim 1's phone number appeared to be spoofed.[3] In the exchange, messages from what appeared to be Victim 1's phone number admit to having an affair with that neighbor's husband. SUBIRANA continued this defamatory narrative through anonymized text messages, including sending one to that same neighbor that said: "Where did the slut tell you she was this weekend?"[4]

9. Over the course of the investigation, the FBI identified another victim of SUBIRANA's cyberstalking campaign, Victim 2.[5] Victim 2 had been in a relationship with SUBIRANA under one of his aliases, Martin KRAKOVICH ("KRAKOVICH"), for approximately four years, officially between September 2016 and January 2020. TextNow records show between November 3, 2016 and September 18, 2021,[6] Victim 2 received

[2] TextNow provides its subscribers internet-based accounts that allow them to use temporarily assigned phone numbers to make phone calls and send, receive, and store messages on the service. TextNow allows users to text and call any number in Canada and the United States. Users are assigned a real phone number which they can use on a smartphone, tablet, or desktop computer that is connected to the internet. TextNow accounts are typically identified by a username, which serves as the subscriber's username. A user's TextNow account also uses an email address or phone number for registration purposes.

[3] Spoofing is a technique in which the name and mobile number of the original sender is changed to appear to be someone else.

[4] The text message was sent to Victim 1's neighbor (XXX-XXX-5790) by phone number [redacted] on January 31, 2021 at 11:53:45 AM UTC. TextNow records show this number was assigned to TextNow account "steve1988smith" between January 31, 2021 and May 2, 2021. Records further show that TextNow accounts controlled by SUBIRANA sent XXX-XXX-5790 approximately 29 messages between January 5, 2021 and September 4, 2021.

[5] Victim 2's identity is known to the FBI and has not been added to this affidavit to protect her identity.

[6] This is the same eriod of time TextNow subpoena returns covered for SUBIRANA-controlled TextNow accounts relating to the harassment of Victim 1.

approximately 202 text messages[7] from anonymized phone numbers associated with SUBIRANA-controlled TextNow accounts intended to intimidate, shame, or otherwise cause her substantial emotional distress. SUBIRANA also contacted numerous friends and associates of Victim 2 via anonymized phone numbers to defame, and further distress her.

10. SUBIRANA met both Victim 1 and Victim 2 on online dating applications and began harassing each almost immediately via TextNow anonymized phone numbers, among other methods of abuse.

11. In the text messages from SUBIRANA's anonymized phone numbers, SUBIRANA would reference what the victims were wearing that day, who they were with, or where they had been physically located to imply that they were being watched or followed. SUBIRANA would also reach out to victims' friends and associates, including former boyfriends or male acquaintances, and impersonate the victims and incite compromising exchanges.

12. In addition, SUBIRANA sent hundreds of "harassing" text messages via these same anonymized phone numbers to himself on his personal phone number in order to obfuscate his identity as the stalker, further distress the victims, and ingratiate himself with victims by appearing to remain steadfastly supportive of them despite his harassment. At one point, SUBIRANA asked Victim 1: "How many guys do you think would have stuck around after that night you were at the Cape", referring to information the "stalker" sent to him. At another point, SUBIRANA told Victim 2, "You've lied to me since we started this relationship, you've brought [the stalker] into my life. Do you think anyone would have lasted this long?" in order to cause feelings of guilt, loyalty, and gratitude on the part of the victim. SUBIRANA would also occasionally engage the "stalker" over text in defense of the victims and subsequently show the victim, seemingly to demonstrate valor and loyalty.

[7] Victim 2 had two phone numbers that received harassing text messages, XXX-XXX-6814 and XXX-XXX-0195.

13. SUBIRANA registered several TextNow accounts used in furtherance of the harassment with Google email accounts.[8] The TextNow account and/or the Google email account name would often reflect a piece of personal information about the victim – their name, for example, or the name of someone SUBIRANA suspected was a former love interest of the victim. In at least one instance, SUBIRANA created a TextNow account under Victim 1's name with the offensive epithet "slut" appended.

14. Using a selection of these Google email accounts, SUBIRANA would email himself information or photos he could use to further stalk and harass the victims. For example, using his cell phone camera, SUBIRANA took pictures of locations where Victim 2 wrote down her accounts and passwords, including the back of an envelope and a page in a notebook. Based on records provided by Google, SUBIRANA also gained access to Victim 2's iPhone when she was in the shower and took pictures with his cell phone of accounts and passwords she wrote down in the Notes app on her iPhone. SUBIRANA subsequently emailed himself these photos to one of his alias Google accounts. Interviews with Victim 2 confirmed that SUBIRANA was not authorized to have access to her device.

15. As described in further detail below, I believe that the evidence demonstrates the Target Locations are connected to SUBIRANA's ongoing and evolving harassment of his victims. To date, the investigation has revealed at least 46,543 text messages sent from TextNow accounts associated with SUBIRANA that were registered using either a Google email account or were accessed with IP addresses that SUBIRANA owned and controlled at his residence. I further believe that content maintained at the Target Locations will not only further expose the criminal activities undertaken by SUBIRANA to intimidate, scare, shame, and defame victims and their associates but could also reveal additional victims of these activities.

[8] Per TextNow, email addresses used for account registration are not verified. The FBI has obtained records from Google for the email accounts controlled by SUBIRANA and used to register TextNow accounts and confirmed the accounts contained within this affidavit were accessed from SUBIRANA's home IP address(es).

16. Based on my training and experience, records detailing connections and patterns across the TextNow and Google accounts, SUBIRANA's IP addresses, and known victims, I believe that SUBIRANA has been engaging, and continues to engage, in this and/or related conduct from at least November 3, 2016 to the present.

B. SUBIRANA's iPhone Number and Residential IP Address

17. Victims 1 and 2 told the FBI in interviews that SUBIRANA's current telephone number associated with an Apple iPhone was [redacted] and provided the FBI with text communications they received from SUBIRANA using telephone number [redacted]. Law enforcement databases listed SUBIRANA's telephone number as [redacted] and indicated the number was associated with an iPhone. According to records provided by Google, the jason.subirana@gmail.com account used the name "Jason Subirana" and the recovery phone number for the account was [redacted] According to records provided by Apple, the jason.subirana@gmail.com account was used to create an Apple account with the telephone number [redacted]. Based on my training and experience, interviews, law enforcement databases, and records produced from providers, I believe SUBIRANA controls the email account jason.subirana@gmail.com, the telephone number [redacted], and the Apple account registered with jason.subirana@gmail.com.

18. Based on records obtained from Comcast, SUBIRANA has a Comcast account at [redacted], Dover, New Hampshire, 03820, associated with the telephone number 603-841-0319. Records from Comcast indicate the IP addresses 73.61.92.86 and 2001:0558:6017:016D:1D62:9B51:02D3:EBAD were assigned to his account from at least as early as March 15, 2021 to August 23, 2021. Additionally, the IP address range[9]

[9] An IP address range is a series of concurrent IP addresses. In this case, any IP address which falls in the assigned range by Comcast would be belong to SUBIRANA's account. For example, for the IP address range assigned to SUBIRANA's account, 2601:0187:8081:5970:0000:0000:0000:0000 to 2601:0187:8081:597F:FFFF:FFFF:FFFF:FFFF, IP address 2601:0187:8081:**5971**:0000:0000:0000:0000 would be in this IP address range, but IP address 2601:0187:8081:**5980**:0000:0000:000:0000 would not.

2601:0187:8081:5970:0000:0000:0000:0000 to 2601:0187:8081:597F:FFFF:FFFF:FFFF:FFFF was assigned to SUBIRANA from March 15, 2021 to August 23, 2021.

19. Based on records obtained from Comcast, SUBIRANA had an additional Comcast account at [redacted], Dover, New Hampshire, and the telephone numbers 603-343-4563 and 603-841-0319. Records from Comcast indicate that the IP addresses 73.61.65.172 and 2001:0558:6017:016D:30BD:B73B:95DA:C0A4 were assigned to this account from at least as early as April 2, 2021 to August 23, 2021. Additionally, the IP range 2601:0187:807F:01A0:0000:0000:0000:0000 to 2601:0187:807F:01AF:FFFF:FFFF:FFFF:FFFF was assigned to SUBIRANA from April 2, 2021 to August 23, 2021.

20. I know from both Comcast and conversations with other law enforcement officers that Comcast only maintains records for the last six (6) months. Therefore, it is possible and, in this case likely, SUBIRANA used these IP addresses prior to the time presented by Comcast. Based on my training, experience, and examination of records to this point, I believe SUBIRANA was assigned these IP addresses some time before the Comcast records indicate.

21. Records from the New Hampshire Department of Motor Vehicles ("DMV") show SUBIRANA's residence was [redacted], Dover, New Hampshire, 03820. Law enforcement database checks also corroborated SUBIRANA lived at [redacted], Dover, New Hampshire, 03820. Records produced by Apple indicated the jason.subirana@gmail.com iCloud account was associated with IP addresses assigned to SUBIRANA's home Comcast account more than 10,000 times from a period of September 4, 2020 to December 24, 2021.

C. **SUBIRANA'S TextNow Accounts**

22. On October 13, 2021, U.S. Magistrate Judge Andrea K. Johnstone authorized a search warrant for nine (9) TextNow accounts the FBI connected to SUBIRANA: [redacted]8588, [redacted]slut, [redacted], [redacted]709, [redacted]66252, [redacted]2068,[redacted], martin_tk, and steve1988smith. As described in the affidavit submitted in support of that search

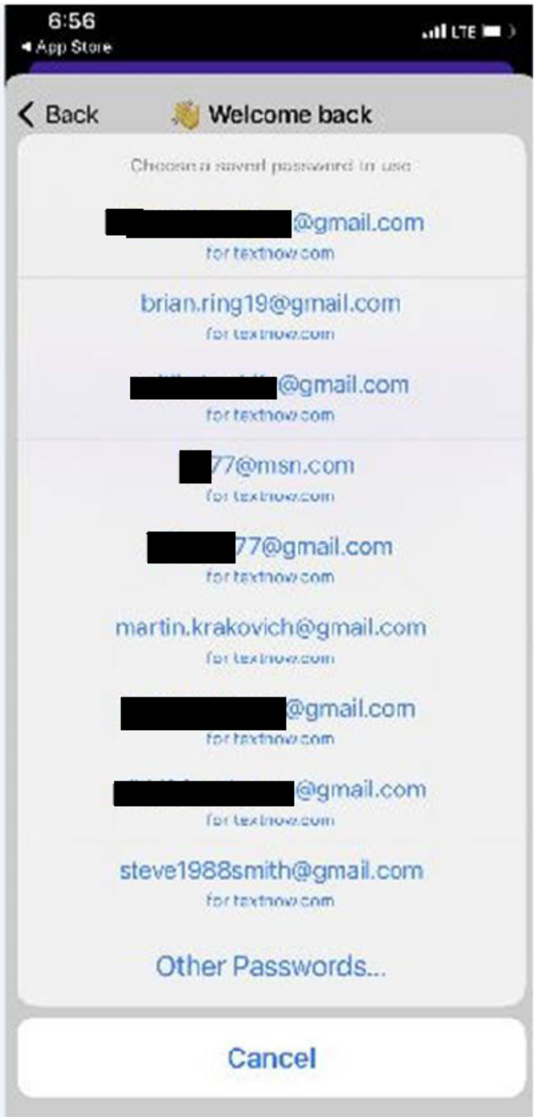
warrant, the FBI's investigation uncovered evidence demonstrating that SUBIRANA controls and uses each of the nine TextNow accounts and that all the accounts had been used in furtherance of the criminal conduct described herein

23. According to records provided by TextNow, approximately 46,543 text messages were sent from approximately 98 different phone numbers assigned to SUBIRANA's known TextNow accounts between February 9, 2016 and October 14, 2021.

24. All nine (9) TextNow accounts were associated with the IP address 73.61.92.186, SUBIRANA's residential IP address, through account registration, access, or email account usage. Specifically, the [redacted], [redacted]slut, [redacted]66252, [redacted], and [redacted]2068 TextNow accounts, which sent victims at least 249 harassing messages between January 9, 2021 and September 29, 2021, were registered using the IP address 73.61.92.186. Furthermore, the [redacted]8588, [redacted]709, steve1988smith, [redacted]slut, [redacted], and [redacted]66252 TextNow accounts accessed the IP address 73.61.92.186 approximately 55 times between May 30, 2021 and August 18, 2021, during which time those accounts sent approximately 57 messages in furtherance of the harassment. The martin_tk TextNow account, which sent approximately 24 messages to Victim 1 between December 10, 2020 and June 4, 2021, was registered using martin.krakovich@gmail.com. According to records from Google, the martin.karakovich@gmail.com email account used IP address 73.61.92.186 or the range 2601:0187:8081:5970:0000:0000:0000:0000 to 2601:0187:8081:597F:FFFF:FFFF:FFFF:FFFF assigned to SUBIRANA's residence to log in approximately 50 times between December 10, 2020 and June 1, 2021.

25. Records provided by Apple revealed a screenshot contained in SUBIRANA's iCloud account that displayed a list of TextNow accounts for which a password had been saved. The list included TextNow accounts registered by the emails [redacted]@gmail.com, martin.krakovich@gmail.com, and steve1988smith@gmail.com, which were all TextNow accounts known to the FBI to be controlled by SUBIRANA. The screenshot also contained options to log into additional TextNow accounts with saved passwords registered with

brian.ring19@gmail.com, [redacted]@gmail.com,[redacted]77@msn.com, [redacted]77@gmail.com, [redacted]@gmail.com, and [redacted]@gmail.com, which were all TextNow accounts previously unknown to the FBI.



Choose a saved password to use

[redacted]@gmail.com
for textnow.com

brian.ring19@gmail.com
for textnow.com

[redacted]@gmail.com
for textnow.com

[redacted]77@msn.com
for textnow.com

[redacted]77@gmail.com
for textnow.com

martin.krakovich@gmail.com
for textnow.com

[redacted]@gmail.com
for textnow.com

[redacted]@gmail.com
for textnow.com

steve1988smith@gmail.com
for textnow.com

26. Based on my training and experience, it is highly likely that the additional accounts listed were used in furtherance of and will contain more evidence of SUBIRANA's criminal activity.

D. SUBIRANA's Google Accounts

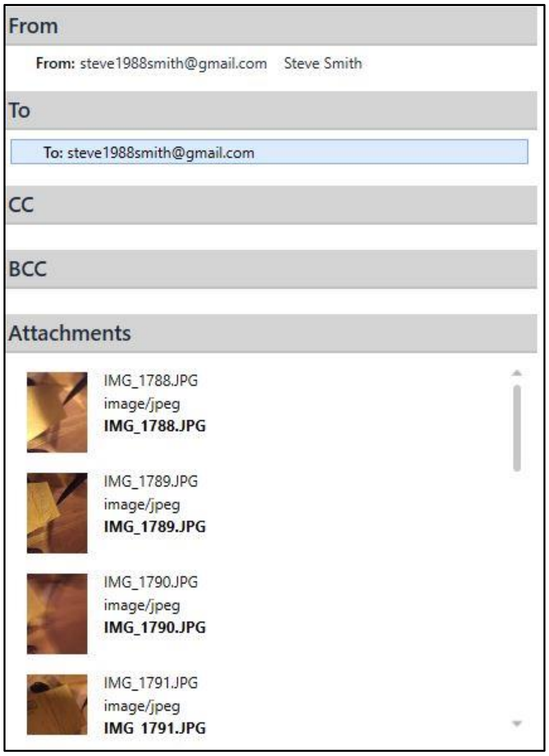
27. On December 23, 2021, U.S. Magistrate Judge Daniel J. Lynch authorized search warrants of five (5) Google accounts tied to SUBIRANA: jason.subirana@gmail.com (the "jason.subirana account"), martin.krakovich@gmail.com (the "martin.krakovich account"), steve1988smith@gmail.com (the "steve1988smith account"), [redacted]@gmail.com (the [redacted] account"), and [redacted]@gmail.com (the [redacted] account").[10] As described in the affidavit submitted in support of those search warrants, the FBI's investigation uncovered evidence demonstrating that SUBIRANA controls and uses each of the five Google accounts and that all the Google accounts had been directly linked to TextNow accounts utilized in furtherance of the criminal conduct described herein.

28. Records provided by Google in response to the search warrants, as described below, demonstrate that SUBIRANA used each of the accounts in furtherance of his criminal conduct with respect to the original known victims, as well as to additional victims.

29. On January 20, 2017, the steve1988smith account sent itself an email with the subject "Envelop" that contained approximately eleven (11) photos of an envelope with several of Victim 2's accounts and passwords written on it. On March 3, 2017, the steve1988smith account sent itself approximately five (5) photos of Victim 2's cell phone screen displaying several of her accounts and passwords in her Notes app. On March 7, 2017, the steve1988smith account sent itself a photo of a "notes" page in a calendar that contained a list of Victim 2's handwritten accounts and passwords. Metadata shows all the aforementioned photos that were emailed from and to the steve1988smith were taken using an iPhone. During follow-up interviews with Victim 2, the FBI confirmed the accounts and passwords belonged to Victim 2 and she did not give them out to anyone, including SUBIRANA. The investigation also confirmed SUBIRANA and Victim 2 were physically together on January 20, March 3, and March 7, 2017.

[10] The affidavit submitted in support of the applications for those search warrants is annexed hereto and incorporated by reference.

Example of photos of Victim 2's passwords emailed from and sent to the steve1988smith account.



From

From: steve1988smith@gmail.com Steve Smith

To

To: steve1988smith@gmail.com

CC

BCC

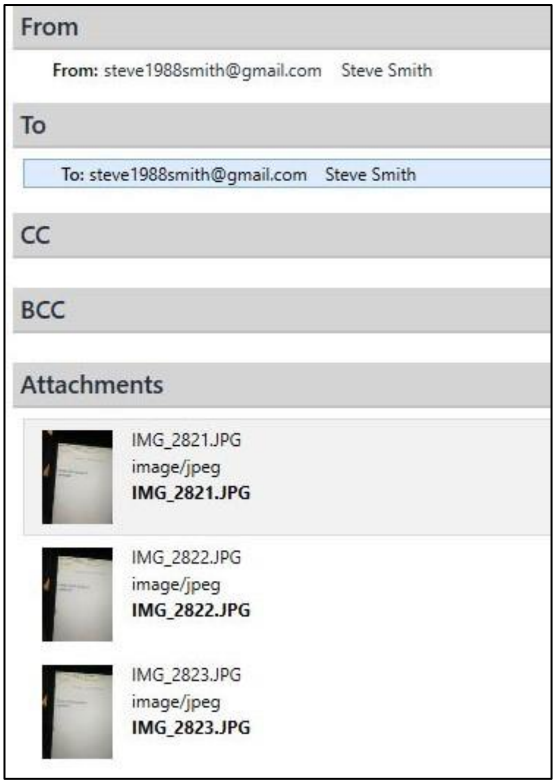
Attachments

IMG_1788.JPG
image/jpeg
IMG_1788.JPG

IMG_1789.JPG
image/jpeg
IMG_1789.JPG

IMG_1790.JPG
image/jpeg
IMG_1790.JPG

IMG_1791.JPG
image/jpeg
IMG 1791.JPG



From

From: steve1988smith@gmail.com Steve Smith

To

To: steve1988smith@gmail.com Steve Smith

CC

BCC

Attachments

IMG_2821.JPG
image/jpeg
IMG_2821.JPG

IMG_2822.JPG
image/jpeg
IMG_2822.JPG

IMG_2823.JPG
image/jpeg
IMG_2823.JPG

30. On March 3, 2017, the steve1988smith account received an email forwarded from Victim 2's personal email account. On May 28, 2017, the steve1988smith forwarded that email to the [redacted] account. Also on May 28, 2017, the [redacted] account forwarded that email back to Victim 2 with the intention of causing her severe emotional distress. The [redacted] account made Victim 2 aware that the email had been forwarded from her own account by someone other than her and without her consent. In addition, the email contained information that SUBIRANA, as her boyfriend, used to manipulate her during their relationship. After Victim 2 did not divulge the existence of the email to SUBIRANA, her boyfriend, the steve1988smith account forwarded the email to the martin.krakovich account on June 7, 2017. SUBIRANA then sent the email he received from the steve1988smith "stalker" account to Victim 2 to demonstrate the "stalker" had passed him information that Victim 2 had withheld.

31. Google search history associated with SUBIRANA-controlled accounts displayed research into topics related to the criminal activity. For example, the jason.subirana account searched "phone spoof app" and visited "SpoofCard: Spoof Calls & Change Your Caller ID" on January 14, 2021, and Victim 1's neighbor received mail appearing to reflect the use of a phone spoofing mechanism on March 3, 2021. In addition, jason.subirana search history demonstrated the following phone tracking and identification inquiries: "can 2 devices have the same ip address", "what imei logged into my gmail account",[11] "can you check imei gmail", "imei number tracker", "imei number", and "cellphone id number". This search history activity indicates SUBIRANA's potentially sophisticated understanding of cell phone and email account connections and tracking via IMEI. The jason.subirana account also searched for "iphone location history" and "iphone location sharing" on December 20, 2020. Between at least October 15, 2020, and April 12, 2021, the jason.subirana account engaged in approximately 24 searches involving the name of Victim 1 or people associated with Victim 1, their addresses, or locations.

32. On November 3, 2016, Victim 2 received the first series of messages from an anonymous number, assigned to the steve1988smith TextNow account, claiming to be a "Steve" she had met at an event the night before. Victim 2 questioned, "Steve from Wanderlush?" at 14:48:50 UTC. The steve1988smith Google search history reflected a search for "Wanderlush" on November 3, 2016 at 14:56:09 UTC. TextNow records showed Victim 2 and SUBIRANA were also texting at the same time "Steve" was texting Victim 2. Victim 2 did not reveal her interaction with "Steve" nor did she mention Wanderlush to SUBIRANA at that time.

33. Google records indicated the jason.subirana, steve1988smith, and the martin.krakovich accounts were all accessed from numerous devices, including, but not limited to, numerous iPhones, an iPad, and a Windows machine. Based on my training and experience, I know that users can log into their Google account(s) through any number of internet-connected

[11] The International Mobile Equipment Identifier (IMEI) is a unique number which identifies mobile phones as well as some satellite phones. Networks use the IMEI to identify valid devices which allows the device to access the network. An IMEI is 15 digits in length and can be identified within a user's phone.

devices. This type of activity gives users the capability to export or save data to any device they use to log into their Google accounts. Based on this information there is probable cause to believe data of evidentiary value resides on any number of devices used to access these Google accounts.

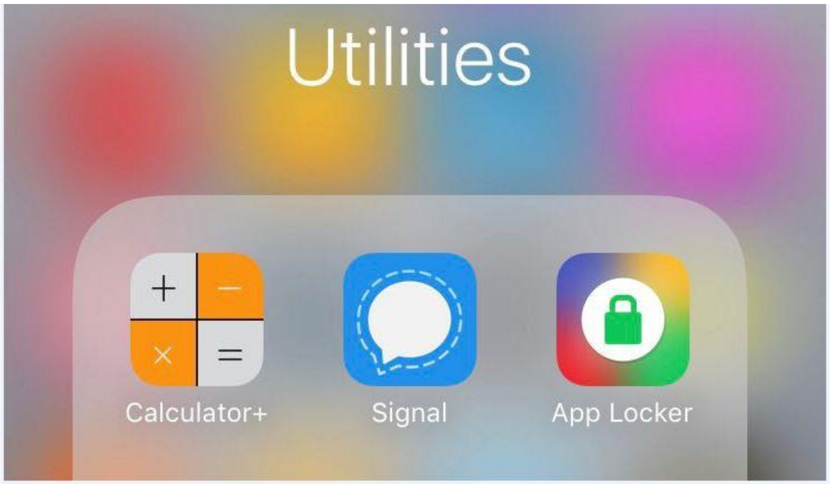
E. SUBIRANA'S iCloud Account

34. On December 23, 2021, U.S. Magistrate Judge Daniel J. Lynch authorized a search warrant of SUBIRANA's iCloud account associated with jason.subirana@gmail.com. Records produced by Apple indicated the iCloud account registered as early as 2011 with the jason.subirana@gmail.com account and identifying number (DSID) 191935685 used the name "Jason Subirana", telephone number [redacted] and the address [redacted], Dover, New Hampshire, 03820. According to Law Enforcement databases, this was a previous address for SUBIRANA. The jason.subirana@gmail.com iCloud account was accessed from numerous devices including, but not limited to, an Apple iWatch, iPad, and numerous iPhones.

35. SUBIRANA's iCloud records included a text conversation in which SUBIRANA admitted to having a media storage application that appeared to be a calculator. SUBIRANA's iCloud records also contained a partial screenshot of an iPhone home screen depicting a "Calculator +" application. Also present in the screenshot was an "App Locker" application, which can be used to secure sensitive applications on a device. Based on my training and experience, conversations with other Agents, and data identified in SUBIRANA's iCloud return,[12] it is likely that SUBIRANA has saved communications, images, or other evidence, fruits, and instrumentalities of criminal activity in secure storage applications on his device. Some of these applications can also be backed up to cloud-based storage such as iCloud or Dropbox.

[12] In addition to App Locker and Calculator +, Apple records indicated SUBIRANA used an application called "Lock My Folder" to store data. This included, but is not limited to, images and videos of victims and potential victims, screenshots of contact information of victims' friends and associates who were later stalked, screenshots of content later used to harass victims, screenshots of TextNow accounts used to harass victims, victim passwords, and other credentials.

Screenshot depicting Calculator+, Signal, and App Locker applications.



36. The screenshot identified above, derived from the Apple search warrant returns from jason.subirana@gmail.com, also included an icon for the messaging application Signal.[13] Based on my training and experience, I know that Signal is used to communicate between parties in an end-to-end encrypted format by default. Frequently the only way investigators are able to obtain the decrypted content of these messages is to obtain the device on which the messages are present. In this case, Signal messages sent and received by SUBIRANA would only be present on the devices on which SUBIRANA used the application (i.e., his iPhone).

37. Based on my training and experience, conversations with other Agents, and information from Apple, I know that iCloud does not back up all data from devices, cellular or otherwise. For example, the jason.subirana@gmail.com iCloud account for which the FBI obtained a search warrant did not contain all data backed up to SUBIRANA's iCloud. I know this because records from Apple indicated not all iCloud features were activated on the jason.subirana@gmail.com account. Based on productions from Apple, iCloud features can be turned on and off at any time by the user. Therefore, the iCloud production provided by Apple may not be comprehensive of all criminal activity present on the device. Based on this fact,

[13] Signal is a messaging application that was developed for users to send messages which are encrypted by default. These messages can include text, files, audio files, images, and video files.

coupled with knowledge obtained from interviews that SUBIRANA was constantly on his iPhone, it is likely that evidence, fruits, and instrumentalities of criminal activity are stored locally on SUBIRANA's device or in other applications or storage media unknown to the FBI.

SUBIRANA'S RESIDENCY AT TARGET LOCATION

38. Over the course of the FBI's investigation, SUBIRANA's residence was determined to be [redacted], Dover, New Hampshire, 03820. According to victim interviews conducted by the FBI, as well as electronic communications records obtained through search warrants, SUBIRANA lives alone at his residence apart from regular visits by his two young children, ages 11 and 13.

39. On March 15, 2022, an FBI Task Force Officer (TFO) conducted surveillance at the Target Location. At approximately 4:00 PM, the FBI TFO observed one of SUBIRANA's vehicles parked on the driveway of the Target Location. The vehicle was a blue-gray Infiniti with New Hampshire license plate number [redacted], which, according to law enforcement records, was registered to SUBIRANA as recently as September 30, 2021.

40. Records obtained from Google for SUBIRANA's jason.subirana@gmail.com account indicated SUBIRANA lives at the Target Location. Homeowner's Association communications for the neighborhood, Amazon and other shipping confirmations to the Target Address, and other various services' quotes and invoices for the Target Address were present in the jason.subirana@gmail.com account, thus confirming SUBIRANA's residence at the Target Location.

41. Based on my training and experience as an FBI Special Agent, as well as through conversations with other members of law enforcement, I know that people engaged in criminal activity, especially criminal activity that involves the use of electronic devices to send text-based messages and images, utilize social media accounts, dating applications, and other messaging and storage platforms, frequently possess evidence of that criminal activity on cell phones. Data relating to such communications, files, and conduct, as well as myriad types of additional

evidence, including internet search history, dating application activity, and social media activity, is frequently stored on cell phones. In this case, SUBIRANA is known to have used one or more cell phones to, among other things, communicate with victims and potential victims in furtherance of his criminal conduct, create and maintain numerous dating application profiles and other social media accounts under various aliases, track at least one victim's location, store private photos or videos taken and/or kept without consent of victims, and transmit harassing text messages to victims. I also understand that people regularly possess cell phones and other electronic devices on their person and in their homes.

42. Based on my training and experience as an FBI Special Agent, as well as through conversations with other members of law enforcement, I understand that people engaged in criminal conduct, especially the criminal conduct described herein, regularly use other electronic devices, including desktop computers, laptop computers, tablet devices, and storage media, in furtherance of their criminal conduct. For example, people use these devices to communicate with victims, store records, files, and images, access email, social media, and dating services accounts, and conduct research regarding particular people, locations, and conduct. I understand that people frequently keep phones, computers, and other electronic devices in their homes. I also understand that people frequently keep phones, computers, and other small electronic devices on their person.

43. Based on Apple search warrant returns, I know that SUBIRANA has had his cellular device with him while in his vehicles. SUBIRANA works from both his home and a commercial office in a neighboring town. Based on my training and experience, I know that people often store any number of devices in their cars. I know that cell phones, thumb drives, and other storage media can be hidden not only in one's residence or on one's person, but also in one's vehicles. It is reasonable to believe that SUBIRANA could store or hide devices and other evidence in his vehicles.

44. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called

"Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly.

45. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

46. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

47. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents.

48. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

49. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked, or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

50. Based on the information provided in this affidavit I believe that SUBIRANA is the primary user of [redacted]. In light of the foregoing, and with respect to (1) any device found on SUBIRANA, or (2) any device that may be seized from [redacted], Dover, New Hampshire, or SUBIRANA’s vehicles based on a warrants approved by this Court based on this affidavit, law enforcement personnel seek authorization, during execution of this search warrant, to: (1) press or swipe the fingers (including thumbs) of SUBIRANA to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of SUBIRANA and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face

of SUBIRANA and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

51. The proposed warrant does not authorize law enforcement to compel that an individual present at any of the residence authorized for search based on this affidavit state or otherwise provide the password or any other means that may be used to unlock or access a device. Moreover, the proposed warrant does not authorize law enforcement to compel an individual present at any of the residence authorized for search based on this affidavit to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

52. Based on my training and experience as an FBI Special Agent, I know that digital evidence tends to be retained on devices and is likely to remain on those devices even if efforts were made to delete or remove that evidence. For example, when a user deletes data from a computer, the data or remnants of the data often remains on that device until overwritten. Even after files have been deleted, they can be recovered months or years later using forensic tools. The investigation to date revealed that SUBIRANA unknowingly retained deleted data (images, video, and texts) from victims with whom he had prior relationships over many years, thus indicating he is likely to maintain additional content on his devices.

53. Based on my training and experience as an FBI Special Agent, through conversations with other members of law enforcement, and through my participation in the investigation described in this affidavit, I understand that people who engage in criminal conduct like cyberstalking may possess hard-copy documents and records, including, but not limited to, online account names, usernames, and passwords, photographs, schedules, and notes associated with victims' family and friends, and that such individuals regularly possess such documents and records on their person, in their homes, and in their vehicles.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

54. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through email, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

55. Based on my training and experience, as well as through information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device.

56. I am aware of a report from the U.S. Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband internet subscription. Specifically, in 2016, when the use of smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone; 58 percent of households had a tablet; and 77 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cellphone, and 81 percent own a cellphone with significant computing capability (a "smartphone").

57. Based on my knowledge, training, and experience, as well as on information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the internet are sometimes automatically downloaded into a temporary internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crimes under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

g. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

58. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence – storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis onsite.

b. Technical requirements – analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden" deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

59. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in these warrants is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of these warrants. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it on-site or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

60. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence described in Attachment B. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

61. These warrants authorize a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to these warrants in order to locate evidence, fruits, and instrumentalities described in these warrants. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to these warrants, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CONCLUSION

62. Based on the foregoing, as well as my training and experience and consultation with other special agents and law enforcement officers, I have probable cause to believe that property constituting evidence of the commission of the Target Offenses, contraband, fruits of crime, or things otherwise criminally possessed, and property designed or intended for use or which is or has been used as a means of committing the Target Offenses will be found at [redacted], Dover, New Hampshire, 03820, as described in Attachment A-1, on SUBIRANA’s person, as described in Attachment A-2, and in SUBIRANA’s vehicles, as described in Attachments A-3, A-4, and A-5.

Sworn to under the pains and penalties of perjury.

/s/ Laura Macrorie
LAURA MACRORIE
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to via telephone in accordance with
Fed. R. Crim. P. 4.1 on April 4, 2022.

Andrea K. Johnstone

HON. ANDREA K. JOHNSTONE
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF NEW HAMPSHIRE